ANALYST CONNECTION

*Sponsored by: Splunk*

**Digital infrastructures are becoming more and more complex every year. The introduction of generative AI will drive even more complexity, and potentially more security concerns, into the institution's environment, threatening the organization's trusted relationship with customers.**

# How Financial Institutions Maintain Customer Trust Despite Security Threats

*July 2024*

**Questions posed by:** Splunk

**Answers by:** Jerry Silva, Program Vice President, IDC Financial Insights

## Q. What is happening in the financial services industry that keeps security teams up at night?

**A.** So much is going on, and has been for years now, that it's hard to pinpoint one thing alone that is potentially threatening the most valuable "product" the institution offers — trust. Once the institution began using the internet to conduct business, bad actors had a new channel, a new attack vector, they looked to exploit. That's not to say that these vulnerabilities didn't exist prior, but the advent of the internet, and more recently cloud, exposed more surfaces that could be attacked, forcing institutions to focus on security — and by extension, data privacy — like they had never done before. Jump to today, and the headlines point to incessant attacks on financial institutions every day. Some large banks, for instance, detect thousands of attempted attacks on their networks every day. Ransomware incidents are on the rise, and the next big threat, in my mind, is an attack vector called "harvest now, decrypt later," where bad actors breach the institution's data and then archive it waiting for quantum as a service to break the encryption on the data and use it to threaten the bank.

So, bottom line, the increased complexity of the institution's digital infrastructure, its on-premise datacenter, multiple cloud providers, third-party business partners, local and remote data stores, and its devices at the edge all add up to a massively complex environment that has to be resilient, scalable, and secure. If we look at generative AI as an example of the latest introduction of a new technology in the industry, institutions now face a new cadre of solutions, platforms, partners, and data sources that will further increase the infrastructure's complexity and expose more security weaknesses.

## Q. There seems to be increased focus on AI, data operations, and the continued move to cloud. Given how institutions feel about security, why would they knowingly create a more complex technology environment?

**A.** The financial institution has to balance four seemingly competing directives. The first one is to provide new products and services to its customers so that the bank customer, insurance client, or investor have the most modern tools to manage

their financial life. This means investing in new technologies, like generative AI, to enable new functionality that will benefit the customer. The second goal is for the institution to successfully compete in the market against peers and/or new entrants into the market. The fintech market is a good example of a completely new IT segment that sprang up in 2010 or so and began eating away at traditional financial institution business by offering new, often better technology than the institution could. Therefore, the institution has to invest in new capabilities sometimes just to keep up, if not to actually create a differentiated edge against competitors.

These business objectives must be balanced with the trust its customers demand from the institution. If an institution's data is breached, or an individual's accounts are taken over and drained, the institution risks losing those customers. This is the third directive and speaks to the previous contention that trust is the number 1 product the institution offers. Finally, financial services is one of the most highly regulated industries in the world. As such, regulation mandates that security and privacy are table stakes and must-haves. The cost of weakness in this case are fines the institution must pay in the event of a security breach, with the secondary effect of stealing investments from the lines of business. Recent operational resilience regulations in the United Kingdom, the EU, and other regions and countries, and those beginning to emerge in Canada increase the importance of security in the broader landscape of business continuity.

This balance is what institutions seek every day. In IDC's April 2023 *CloudPath Survey,* security was the top factor institutions considered before moving a workload to cloud. In IDC's November 2023 *North American Banking Survey,* security and privacy/compliance were the top challenges for banks in implementing data operations. So, while innovation from the business is needed for growth, security continues to be the overriding consideration for the organization. The real magic here is how the institution can improve its security without negatively impacting innovation, the customer experience and, ultimately, trust in the industry.

## Q. You said those are "seemingly" competing directives. Is there a business benefit to improving the institution's security posture?

**A.** Absolutely, but it takes an enterprise approach to security as a business strategy. If the institution manages to demonstrate a strong security capability to its customers and avoid an undue burden on the customer to comply with overly strenuous security controls, it will continue to maintain its customer base and grow it through secure convenience. This is especially important for the institution's business clients, small business, and corporations. This same security capability can be a differentiating factor in the market.

Having an enterprise security strategy should mean the number of security incidents will decrease. After all, it's not reasonable to believe that an institution will be guaranteed to avoid any security lapse. But anything the institution can do to minimize the costs associated with security, again by having an enterprise approach and avoiding duplication of expenses, can allow it to direct more investments to line-of-business innovation. The same holds true if the institution can steer clear of regulatory fines and costs of restitution for security breaches.

Cost avoidance is especially important when new technologies like generative AI are adopted. In IDC's December 2023 *Future Enterprise Resiliency and Spending Survey,* 31% of financial institutions cited they would aggressively cut spend in other areas to fund investments in generative AI. Not only can areas like security not be cut but increased investments in security can actually free up funds so that business areas don't have to be sacrificed to fulfill investments in innovation.

## Q. What do you think is the institution's biggest challenge in accomplishing what you just described as the business benefits of security?

**A.** Just as is the case in most, if not all, circumstances of transformation, the culture and the established roles within the institution often have to change to accommodate new ways of thinking. This is especially true in IT as the entire digital infrastructure expands to enable new technologies and open roads to innovation. More and more of the institution's focus needs to be on managing and governing technology, as opposed to creating or building technology. This isn't always true, especially at larger institutions that believe, and rightly so, that their own technology capabilities provide competitive differentiation. But at the majority of financial institutions worldwide, the simple fact is that the organization is finding it difficult, and at times impossible, to find and maintain the number of skill sets they need to keep abreast of technological innovation, including how to implement innovative technologies while maintaining security. The risk here is that through a lack of appropriate security skills, the institution cannot ensure the level of security it must have.

This is where financial institutions are relying more and more on external partners, whether in infrastructure, software, or services, that are better able to support technologies like security. These partners are experts in their domain, can find the right people to build and maintain security systems, supply tools to continue to monitor and maintain, and provide these to the institution as platforms or services. By leveraging these partners, the institution has to shift its focus from building to managing the partners and governing the process and compliance of any security platform. This requires a cultural shift and a large change of mindset of the risks of using external providers for something as important as its security posture.

## Q. What do you tell your institution clients about improving their security? Where should they start?

**A.** That cultural and mindset shift from "do it myself" to using external security partners has to start at the very top of the organization. The business value from using a third-party provider to ostensively improve the institution's security capabilities, again with the customer experience in mind, must be defined to defend the investment and time it will take the organization itself to refocus on governance, risk, and compliance instead of building and operating security platforms. This has to be the first step. For those institutions that have already addressed the organizational changes needed, they can begin to look for partners that fit into the organization and its needs in the market.

Second, the historic and notoriously siloed nature of most finance institutions isn't limited to the lines of business. As platforms have been introduced over time, and as the digital infrastructure continues to expand, the security environment has become fragmented as well, including staff, data, and systems. Security needs to be an enterprise capability across all lines of business and architectures. Bringing all resources, internal and external, into one enterprise security strategy is key to ensuring trust.

At that point, the implementation of security will be a process of progressive modernization that will take time. The institution can choose to deploy new security functionality based on return, the "biggest bang for the buck," or risk, with the lowest risk processes or platforms chosen first as production proof of concepts before implementing in other areas.

In all cases, security will require a rethinking of the institution's role in creating a security stance that improves the customer experience, creates a competitive advantage, frees funds for investment in innovation, all while leveraging expert providers that can arguably provide better security than the institution itself.

# About the Analyst

***Jerry Silva,*** *Program Vice President, IDC Financial Insights*

Jerry Silva is vice president for IDC Financial Insights responsible for the global retail banking practice. Jerry's research focuses on technology trends and customer expectations and behaviors in retail banking worldwide. Jerry draws upon over 35 years' experience in the financial services industry to cover a variety of topics, from the back office to customer channels to governance in the technology shops at financial institutions. His work for both institutions and vendors gives Jerry a broad perspective in technology strategies.

## MESSAGE FROM THE SPONSOR

**Building Digital Resilience in Financial Services**

Financial service institutions are some of the most data-intensive and heavily regulated organizations and are subject to heavy fines for noncompliance. They are also the target of many of the most sophisticated cyberattacks, and much of the world economy depends on financial service institutions staying up and running despite escalating disruptions. The resilience of their digital systems is critical to building a safer and more resilient digital world.

Learn more about the top threats in financial services.

www.splunk.com/fsi.

IDC Custom Solutions

**IDC Research, Inc.**
140 Kendrick Street
Building B
Needham, MA 02494
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com



#US52467424